**Session structure/process**

* As attendees enter, ask them to place sticky-notes on top of their badges, only allowing first names to show and to only introduce themselves by first names.
  + Purposes:
    - Start event with something a bit disruptive
    - Exercise in personal privacy
    - Eliminate unconscious bias based on titles and institutions
    - Provide some institutional privacy when talking about practices
    - Better excuse to continue talking to each other after the session ends
* Begin with context setting of privacy and security
  + Definitions of privacy/security (slides)
  + Mention of national/global debate on privacy and security
  + Walk through recent headlines about privacy and security in higher education (slides)
* Scenario exercises
  + Each table gets slips of paper with six scenarios (below in this document) and is instructed to work in pairs for 4 mins to discuss the worst case scenario of how an institution would handle the scenario.
  + Each table is instructed to discuss what their worst case scenarios had in common/different (4 min)
  + Each table reports out things in common and these are documented on flip-chart.
  + Walk through each scenario asking if there were items that were unique to each one instead of being in common.
  + Participants stand up and switch tables
  + Using the same six scenarios, they are asked to pair up again and discuss the best case process for handling the scenarios (4 min)
  + Each table is instructed to discuss what their best case scenarios had in common/different (4 min)
  + Each table reports out things in common and these are documented on flip-chart.
  + Flip charts are posted on opposite ends of the room and participants are asked to line up between them where they think their institution’s practices are in the spectrum of best to worst case.
* Wrap up
  + Participants are encouraged to learn more about the policies and practices at their institutions in regard to privacy and security intersections.
  + Return to slides for full quote about “no easy answers”

**Scenario 1: Supervisor request for web usage data**

A manager in an administrative department contacts security because they have concerns that an employee is using their work hours for online gambling. They would like you to check into their online habits at work and report back what you find about the employee visiting inappropriate websites.

**Scenario 2: Law Enforcement request for student location**

Campus/local law enforcement gives you a phone call asking if you can provide the current location of a student based on the wireless network and their cell phone. The student’s roommate raised concern of suicidal behavior and they haven’t been able to locate the student.

**Scenario 3: Media request for public records**

You work at a public institution and receive a request from the major regional newspaper for emails between executives regarding a controversial real estate deal to expand the campus. They request the information be provided under the state’s open records law.

**Scenario 4: Student honor code violation investigation**

The student judicial board is reviewing a case of suspected cheating where one student may have paid another to complete an online exam. They would like you to review any available IT information that could prove or disprove the suspected cheating.

**Scenario 5: Threat of violence against community**

An anonymous message has been posted to an internet discussion board threatening a shooting on your campus in six hours. The campus/local police have been alerted to this issue and want to know if it was posted by someone on campus and, if so, who posted it.

**Scenario 6: FBI investigation into faculty member**

You have been contacted by the FBI who is investigating a faculty member suspected of trafficking in child pornography. They want your assistance in setting up special monitoring of the network to verify and document this activity, followed by assistance in locating the individual for arrest.